

# SIMPLE NOTES ON REAL QUADRATIC FIELDS OF MINIMAL TYPE

PARK, JEONGHO

ABSTRACT. The notion of minimal type introduced in [3] is rediscovered in geometric point of view, and it is shown that in a natural way almost all real quadratic number fields are of minimal type, which is another evidence supporting the Gauss conjecture on class numbers.

## INTRODUCTION

In recent years Kawamoto and Tomita introduced a subclass of real quadratic number fields called *minimal type*. They showed several conclusions about fields that are not of minimal type, in particular the validity of Ankeny-Artin-Chowla conjecture and the non-triviality of ideal class group except 51 (and one more possible) exceptions. The great interest on class groups therefore led to the study of minimal types, and in terms of continued fraction, the discriminants of minimal type are classified in the same paper [3] up to period  $l \leq 4$ . The argument in [3] exploits the continued fraction expansion of  $\sqrt{d}$  and its period.

In this paper, however, we appeal to the best approximation property of the convergent  $p_n/q_n$  and examine its approximation quality. In this way we reconstruct the quadratic polynomial given in the aforementioned paper and thereby rebuild the minimal type discriminants in a different formulation, which has an advantage in its flexibility to be generalized as in [4]. We also prove the dominance of minimal types over all discriminants, which is in some sense a negation of the partial proof of AAC conjecture, but is a supporting evidence in the sense of Gauss conjecture.

---

*Date:* November 16, 2012.

*1991 Mathematics Subject Classification.* Primary:11J68, Secondary: 11R29, 11Y40.

*Key words and phrases.* Real quadratic number field, Continued fraction, Minimal type.

Supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (2010-0026473).

## 1. THE ATTACHED INTERVALS

Let  $d > 0$  be a non-square integer and  $\sqrt{d} = [a_0, a_1, a_2, \dots]$  be the simple continued fraction expansion of  $\sqrt{d}$ ,  $l$  its period,  $\frac{p_n}{q_n} = [a_0, a_1, \dots, a_n]$  a convergent,  $\alpha_{n+1} = [a_{n+1}, a_{n+2}, \dots]$  the  $(n+1)$ -th total quotient, and  $N(x)$  the usual norm of  $x \in \mathbb{Q}(\sqrt{d})$ . Put  $\xi_n = p_n + q_n\sqrt{d}$  and let  $\nu_n = |N(\xi_n)| = (-1)^{n+1}N(\xi_n)$ . We say that a quadratic integer  $\xi$  *comes from* a convergent to  $\sqrt{d}$  when  $\xi$  is of this form.

We include a lemma first.

**Lemma 1.0.1** ([4]). (1) For  $n \geq 0$

$$\alpha_{n+1} = \frac{2\sqrt{d}}{\nu_n} - \frac{q_{n-1}}{q_n} + O\left(\frac{1}{q_n^2\sqrt{d}}\right).$$

(2) every quadratic integer in  $\mathbb{Z}[\sqrt{d}]$  whose norm is less than  $\sqrt{d}$  and is square-free comes from a convergent to  $\sqrt{d}$ .

Recall that every irrational number has a unique continued fraction expansion. It is a simple observation that the real line is partitioned by the predecessors, i.e., for any  $a_0, a_1, \dots, a_m$  the set

$$\{x \in \mathbb{R} \mid x = [a_0, a_1, a_2, \dots, a_m, *]\}$$

is a closed interval. Let  $q_t$  be the denominator of  $[0, a_1, a_2, \dots, a_t]$ . The following proposition quantifies these intervals considering  $\sqrt{d}$ .

**Proposition 1.0.2.** Let  $a_1, a_2, \dots, a_m$  be positive integers and  $f(N)$  the number of non-square  $d$ 's between 1 and  $N$  such that

$$\sqrt{d} = [a_0, a_1, a_2, \dots, a_m, *]$$

Then

$$\lim_{N \rightarrow \infty} \frac{f(N)}{N} = \frac{1}{q_m(q_m + q_{m-1})}.$$

We give a sketch of proof. Consider the numbers in the interval  $(n^2, (n+1)^2)$ . The graph  $y = \sqrt{x}$  is almost linear in  $n^2 < x < n^2 + 2n + 1$ , and the difference between  $[n, a_1, a_2, \dots, a_m] = [n, a_1, a_2, \dots, a_m, \infty]$  and  $[n, a_1, a_2, \dots, a_m + 1]$  is  $\frac{1}{q_m(q_m + q_{m-1})}$ . The computation with a proper estimation of the errors that arise from the difference between the graph  $y = \sqrt{x}$  and a straight line is immediate.

Note that

$$N(p + q\sqrt{d}) = p^2 - q^2d = \mu \Rightarrow \left| \frac{p}{q} - \sqrt{d} \right| = \frac{|\mu|}{(p + q\sqrt{d})q},$$

which interprets the norm of a quadratic integer as a measure of how efficient the approximation of  $\sqrt{d}$  by  $\frac{p}{q}$  is. In particular, a quadratic unit appears when this efficiency is the best. Lemma 1.0.1 also shows that  $\xi_n$  becomes a unit if and only if the  $(n+1)$ -th convergent becomes as large as possible, namely  $\alpha_{n+1} > \frac{2\sqrt{d}}{2} + o(\sqrt{d})$ . As can be naturally implied by these, the size of  $\alpha_{n+1}$  directly tells us how close the convergent  $p_n/q_n$  is to  $\sqrt{d}$ .

Based on the above paragraphs, for each finite sequence  $\frac{p}{q} = [a_0, a_1, a_2, \dots, a_m]$  of positive integers we can assign a tiny interval  $I_{p/q}$  that consists of points whose square roots are especially close to  $p/q$ . More specifically, we want this interval to satisfy following property: whenever a non-square integer  $d$  falls into that interval, the efficiency of approximation of  $\sqrt{d}$  by  $p/q$  is the best and  $p + q\sqrt{d}$  becomes a quadratic unit. Explicitly, we can take the interval as

$$I_{p/q} = \left( [a_0, a_1, \dots, a_m, \frac{4}{3}\sqrt{d}]^2, [a_0, a_1, \dots, a_m, 1, \frac{4}{3}\sqrt{d}]^2 \right)$$

(or the reverse of this, according to the parity of  $m$ .)

Write  $\lfloor \frac{p}{q} \rfloor = a_0 = n = \lfloor \sqrt{d} \rfloor$ , so  $I_{p/q}$  is an interval in  $(n^2, (n+1)^2)$  and we are dealing with non-square  $d$  that are in the same range. The factor  $\frac{4}{3}$  in the last entry is chosen somewhat arbitrarily; Since the partial quotient cannot take values between  $\sqrt{d} + \epsilon$  and  $2\sqrt{d} - \epsilon$ , any number between  $1 + \epsilon$  and  $2 - \epsilon$  will be fine.

We denote the fractional part of  $p/q$  by  $\{p/q\} = k/q$ .

**Theorem 1.0.3.**  *$I_{p/q}$  contains an integer if and only if*

$$k^2 \equiv -1 \pmod{q}, \quad 2n \equiv k \left( \frac{1+k^2}{q} \right) \pmod{q}$$

or

$$k^2 \equiv 1 \pmod{q}, \quad 2n \equiv k \left( \frac{1-k^2}{q} \right) \pmod{q}$$

and in that case the integer  $d$  contained in  $I_{p/q}$  is given by

$$d = n^2 + 2\frac{k}{q}n + \frac{k^2 \pm 1}{q^2}.$$

*Proof.* Assume  $m$  is even. Then

$$\begin{aligned}
& \text{The interval } \left( \frac{p^2}{q^2}, [n, a_1, \dots, a_m, \frac{4}{3}\sqrt{d}]^2 \right) \text{ contains an integer} \\
& \Leftrightarrow \left\lceil \frac{p^2}{q^2} \right\rceil - \frac{p^2}{q^2} < \frac{1.5}{q^2} \\
& \Leftrightarrow \left\{ \frac{p}{q} \right\}^2 + 2n \left\{ \frac{p}{q} \right\} \pmod{1} \in \left( 1 - \frac{1.5}{q^2}, 1 \right) \pmod{1} \\
& \Leftrightarrow 2n \left\{ \frac{p}{q} \right\} \pmod{1} \in \left( -\frac{k^2}{q^2} - \frac{1.5}{q^2}, -\frac{k^2}{q^2} \right) \pmod{1} \\
& \Leftrightarrow 2nk \pmod{q} \in \left( -\frac{k^2}{q} - \frac{1.5}{q}, -\frac{k^2}{q} \right) \pmod{q} \\
& \Leftrightarrow k^2 \equiv -1 \pmod{q}, 2n \equiv k^{-1} \left( \frac{-1 - k^2}{q} \right) \equiv k \left( \frac{1 + k^2}{q} \right) \pmod{q}
\end{aligned}$$

For odd  $m$ , a similar computation shows that

$$\begin{aligned}
& \text{The interval } \left( [n, a_1, \dots, a_m, \frac{4}{3}\sqrt{d}]^2, \frac{p^2}{q^2} \right) \text{ contains an integer} \\
& \Leftrightarrow k^2 \equiv 1 \pmod{q}, 2n \equiv k^{-1} \left( \frac{1 - k^2}{q} \right) \equiv k \left( \frac{1 - k^2}{q} \right) \pmod{q}
\end{aligned}$$

Recall that a rational number  $p/q$  can have both even or odd length. When this ambiguity is compensated by putting or eliminating 1 at the last entry, the two half-intervals in the computation unifies to  $I_{p/q}$ .

The expression of  $d$  in terms of  $n, k, q$  is of triviality, considering the integer closest to  $(n + k/q)^2 = n^2 + 2nk/q + k^2/q^2$ .  $\square$

## 2. DOMINANCE OF THE MINIMAL TYPES

Choose any pair  $(y, x)$  with  $0 \leq x < y$ ,  $x^2 \equiv 1$  or  $-1 \pmod{y}$ . Let

$$\tilde{y} = \begin{cases} \frac{y}{2} & \text{if } y \text{ is even} \\ y & \text{otherwise} \end{cases}$$

The set of  $n$ 's for which  $I_{n+x/y}$  contains an integer  $d$ , or equivalently, positive  $n$ 's for which an integer  $d$  exists between  $n^2$  and  $(n+1)^2$  such that  $ny + x + y\sqrt{d}$  becomes a quadratic unit, forms an arithmetic progression with common difference  $\tilde{y}$ .

For such pair  $(y, x)$ , let  $\mathfrak{D}(y, x)$  be the set of (non-square) integers  $d$  contained in the intervals  $\{I_{n+x/y}\}_n$  where  $n$  runs through the arithmetic

progression. Let  $x/y = [0, a_1, a_2, \dots, a_m]$ . Then for any  $d \in \mathfrak{D}(y, x)$  we have

$$\sqrt{d} = [\lfloor \sqrt{d} \rfloor, \overline{a_1, a_2, \dots, a_m, 2\lfloor \sqrt{d} \rfloor}]$$

and unless  $2\lfloor \sqrt{d} \rfloor = \max\{a_1, a_2, \dots, a_m\}$  the period is exactly  $m+1$  and  $\lfloor \sqrt{d} \rfloor y + x + y\sqrt{d}$  is the fundamental solution to the Pell's equation  $X^2 - dY^2 = \pm 1$ . It can be easily checked that every solution to this Pell's equation is a power of the fundamental solution even when  $d$  has square factors. Since the partial quotients of  $\sqrt{d}$  cannot exceed  $2\lfloor \sqrt{d} \rfloor$ , such exceptional case can occur only at the least element of  $\mathfrak{D}(y, x)$ . Let  $\overline{\mathfrak{D}}(y, x)$  be the set  $\mathfrak{D}(y, x)$  where this possible exception is removed, i.e., with the least element discarded if its period is less than  $m+1$ . Observe that  $\{\overline{\mathfrak{D}}(y, x)\}_{y,x}$  forms a partition of the set of non-square integers.

Combining the notion of  $\overline{\mathfrak{D}}(y, x)$  and the theorems in [1], [2], and Theorem 3.1 in [3], following proposition is an immediate corollary.

**Proposition 2.0.4.** *Let  $0 \leq x < y$ ,  $\frac{x}{y} = \frac{p_m}{q_m} = [0, a_1, a_2, \dots, a_m]$ ,  $\frac{p_{m-1}}{q_{m-1}} = [0, a_1, a_2, \dots, a_{m-1}]$ , where the parity of  $m$  is uniquely determined by*

$$(q_m, p_{m-1}) \not\equiv (0, 1) \pmod{2}.$$

*Then*

$$\begin{cases} x^2 \equiv 1 \pmod{y} & \Leftrightarrow (a_1, a_2, \dots, a_m) \text{ is symmetric, } m \text{ is odd;} \\ x^2 \equiv -1 \pmod{y} & \Leftrightarrow (a_1, a_2, \dots, a_m) \text{ is symmetric, } m \text{ is even.} \end{cases}$$

If  $d$  is the least element of  $\overline{\mathfrak{D}}(y, x)$  for some  $(y, x)$ , then  $d$  is said to be of *minimal type*, which agrees with the definition of *minimal type* for  $\sqrt{d}$  imposed in [3] in a somewhat different fashion.

A quantification of the integers of minimal type can be found in the following theorem. In an expository manner, it says that almost all non-square positive integers are of minimal type and the proof also shows that  $\overline{\mathfrak{D}}(y, x) = \mathfrak{D}(y, x)$  for almost all  $(y, x)$ .

**Theorem 2.0.5.** *Let  $\overline{\mathfrak{D}}$  be the set of all non-square positive integers of minimal type. Then*

$$\sum_{d \in \overline{\mathfrak{D}}} \frac{1}{d^s} \approx \zeta(s) \quad \text{as } s \rightarrow 1+.$$

(where ' $\approx$ ' means the difference is bounded.)

*Proof.* Let  $d_0(y, x)$  be the least element of  $\mathfrak{D}(y, x)$ , and

$$V(y) = \{x \mid 0 \leq x < y, x^2 \equiv \pm 1 \pmod{y}\},$$

$$I_1 = \{(y, x) \mid y \geq 1, x \in V(y), \overline{\mathfrak{D}}(y, x) = \mathfrak{D}(y, x)\},$$

$$I_2 = \{(y, x) \mid y \geq 1, x \in V(y), \overline{\mathfrak{D}}(y, x) \neq \mathfrak{D}(y, x)\}.$$

We can easily compute the following sums:

$$\begin{aligned}
\zeta(s) - \zeta(2s) &= \sum_{y=1}^{\infty} \sum_{x \in V(y)} \sum_{d \in \bar{\mathfrak{D}}(y,x)} \frac{1}{d^s} \\
&= \sum_{(y,x) \in I_1} \left( \frac{1}{d_0(y,x)^s} + \sum_{k=1}^{\infty} \frac{1}{\left( (\sqrt{d_0(y,x)} + k\tilde{y})^2 + O(1/y^2) \right)^s} \right) \\
&\quad + \sum_{(y,x) \in I_2} \sum_{k=1}^{\infty} \frac{1}{\left( (\sqrt{d_0(y,x)} + k\tilde{y})^2 + O(1/y^2) \right)^s} \\
&= \sum_{(y,x) \in I_1} \left( \frac{1}{d_0(y,x)^s} + \frac{1}{\tilde{y}^{2s}} (\zeta(2s) - O(1)) \right) \\
&\quad + \sum_{(y,x) \in I_2} \frac{1}{\tilde{y}^{2s}} (\zeta(2s) - O(1)).
\end{aligned}$$

$V(y)$  can be divided into  $V^+(y)$  and  $V^-(y)$  where

$$V^+(y) = \{x \mid 0 \leq x < y, x^2 \equiv 1 \pmod{y}\},$$

$$V^-(y) = \{x \mid 0 \leq x < y, x^2 \equiv -1 \pmod{y}\}.$$

Using Chinese remainder theorem and the fact that the group of units modulo  $p^n$  for an odd prime  $p$  is cyclic, it is easy to see that  $x^2 \equiv 1 \pmod{y}$  has  $O(2^{\omega(y)})$  roots. The same is true for  $x^2 \equiv -1 \pmod{y}$  if  $-1$  is a quadratic residue for every prime divisor of  $y$ ; otherwise it has no solutions. It follows that

$$\sum_{y=1}^{\infty} \sum_{x \in V(y)} \frac{1}{y^{2s}} \ll \sum_{y=1}^{\infty} \sum_{x \in V^+(y)} \frac{1}{y^{2s}} \ll \sum_{y=1}^{\infty} \frac{2^{\omega(y)}}{y^{2s}} = \frac{\zeta(2s)^2}{\zeta(4s)} = O(1)$$

and therefore

$$\sum_{(y,x) \in I_1} \frac{1}{d_0(y,x)^s} \approx \zeta(s) \quad \text{as } s \rightarrow 1+$$

which proves the assertion.  $\square$

## REFERENCES

1. C.Friesen, *On continued fractions of given period*, Proc. Amer. Math. Soc (1988), no. 103, 9–14.
2. F.Halter-Koch, *Continued fractions of given symmetric period*, Fibonacci Quart. (1991), no. 29, 298–303.
3. F.Kawamoto and K.Tomita, *Continued fractions and certain real quadratic fields of minimal type*, J. Math. Soc. Japan **60** (2008), no. 3, 865–903.
4. JH.Park, *Notes on the quadratic integers and real quadratic number fields*, Preprint.

DEPARTMENT OF MATHEMATICS (ROOM 117), POHANG UNIVERSITY OF SCIENCE  
AND TECHNOLOGY, SAN 31 HYOGA DONG, NAM-GU, POHANG 790-784, KOREA.  
TEL. 82-10-3047-7793.

*E-mail address:* pkskng@postech.ac.kr